IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

I.C., a minor, by and through his natural parent, NASIM CHAUDHRI, on behalf of himself and all others similarly situated, *Plaintiff,* v. STOCKX, INC.; and STOCKX, LLC, *Defendants*.	Case No. _____ Hon. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

I.C., a minor by and through his natural parent, Nasim Chaudhri, individually and on behalf of a Class defined below of similarly situated minor persons, alleges the following against Defendants StockX, Inc., and StockX, LLC (collectively "StockX") based upon personal knowledge and on information and belief derived from, among other things, StockX's August 8, 2019 "Notice of Data Breach," investigation of counsel, and review of public documents as to all other matters.

NATURE OF COMPLAINT

1. Plaintiff brings this action against StockX for StockX's failure to reasonably safeguard Plaintiff's PII as defined herein, failure to reasonably provide timely notification that Plaintiff's PII had been accessed and acquired by an

unauthorized third party, and for intentionally and unconscionably deceiving Plaintiff relating to the status, safety, location, access, and protection of Plaintiff's PII.

2. As a result of StockX's negligent, intentional, or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff's PII was accessed, acquired, stolen, and re-sold by thieves for the express purpose of misusing Plaintiff's data and causing further irreparable harm to Plaintiff's personal, financial, reputational, and future well-being.

3. Plaintiff brings this lawsuit against StockX for statutory violations as well as common law tort claims under negligence, negligent misrepresentation, fraud and fraud through silence, negligence per se, unjust enrichment, violation of state data breach statutes, intrusion upon seclusion, and declaratory judgment.

4. As used throughout this Complaint, "Personally Identifiable Information" or "PII" is defined as all information exposed by the StockX data breach, includes all information so defined under individual states' statutes, and includes all or any part or combination of name, address, birth date, Social Security number, driver's license information (any part of license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, usernames, passwords, and log-in information that can be used to access a person's personal electronic content.

PARTIES

5. StockX, Inc. is a Delaware corporation with its principal place of business in Detroit, Michigan.

6. StockX, LLC, is a Michigan limited liability company with its principal place of business in Detroit, Michigan.

7. Plaintiff is an individual citizen of Kansas, who had a StockX account at the time of the incidents described herein and entrusted PII (as defined herein) to StockX with the reasonable expectation and understanding that StockX would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users and would be timely and forthright relating to any data security incidents involving Plaintiff's PII.

JURISDICTION AND VENUE

8. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and StockX is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

9. This Court has personal jurisdiction over StockX because it is authorized to and regularly conducts business in Michigan and is headquartered in Detroit, Michigan.

10. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because StockX entered into terms of service and privacy agreements with Plaintiff in Kansas and Michigan, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in Kansas and Michigan.

GENERAL ALLEGATIONS

I. StockX – Background.

11. StockX is an ecommerce platform for luxury goods, fashion clothing, and accessories, with a particular emphasis on ultrarare, custom, vintage, and highly sought shoes for "sneakerheads," including minors.

12. Under StockX's business model, products posted on its platform are treated similarly to the way in which stocks are traded on the market — i.e., each product is assigned a ticker symbol, sellers put out asking prices, and the products are then bid on by prospective purchasers. Users of StockX then see data such as price volatility, highs, and lows from across the internet, and once a bid matches with an

asking price, the sale occurs automatically.[1] StockX then takes a flat commission on each sale ranging from 8–9.5 percent.[2]

13. For example, in January of 2018, StockX sold limited-edition LeBron James shoes for an average of $6,000 per pair—with approximately $500 of each going directly to StockX. The shoes would then be "flipped" on the same StockX marketplace, with StockX, again, realizing its commission, without the purchaser ever taking actual physical possession of the shoes.[3]

14. Some sneakers on StockX have been sold for as high as $30,000, and at one time, the site had sneakers with an asking price of $850,000.[4]

15. StockX has grown rapidly since its inception in February 2016. As of mid-2018, StockX was conducting more than 10,000 transactions per day, had 370 employees, and more than $700 million in sales.

---

[1] https://www.nytimes.com/2018/07/06/business/smallbusiness/stockx-sneakerheads-luxury-goods.html?smid=nytcore-ios-share&module=inline (Last visited, August 2019) (Exhibit 1).
[2] *Id.*
[3] *Id.*
[4] https://www.sportswear-international.com/news/portrait/Marketplace-How-StockX-is-revolutionizing-the-sneaker-reseller-business-online-14099 (Last visited, August 2019) (Exhibit 2).

16. More recently, StockX reported sales of $100 million per month, and in June 2019, StockX raised $110 million in financing (on top of a previous $60 million), valuing it at more than $1 billion and in excess of 800 employees.[5]

II. StockX collects personally identifiable information from its users.

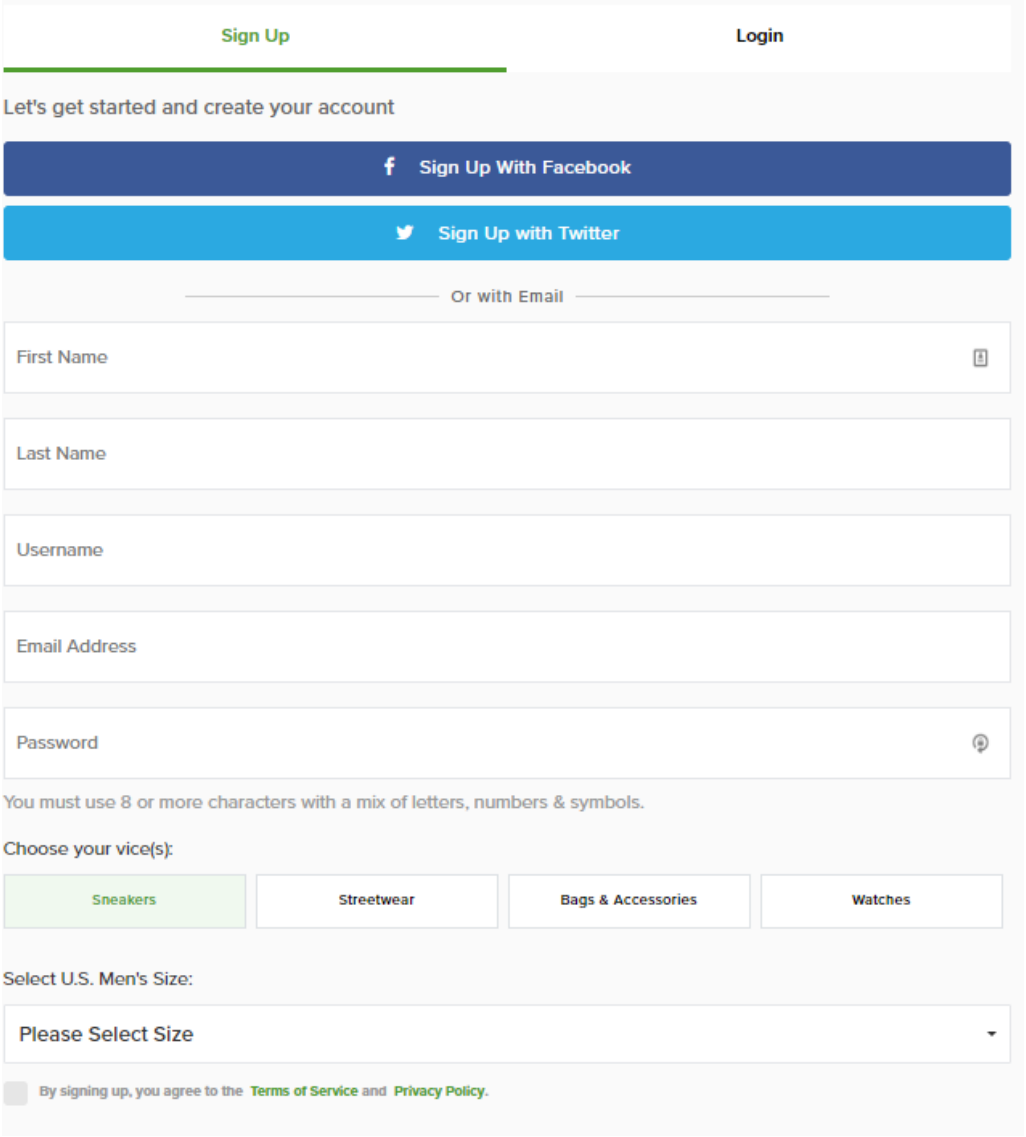
17. StockX requires all individuals who wish to use its platform to create a StockX user account, which requires the prospective user to submit certain information to StockX. The prospective user can create an account with StockX through the user's email address.

18. The information that StockX requires for prospective users to become active users initially includes the user's first name, last name, email address, a username, and a password. The user can then select one or more of four "vices": Sneakers, Streatwear, Bags & Accessories, or Watches. If "Sneakers" is one of the "vices" selected, StockX's sign-up form automatically prompts the prospective user to "Select U.S. Men's Size" by choosing from a drop-down box.

19. At the bottom of the Sign Up form, StockX includes a single-line checkbox advising prospective users that by signing up for their service they must agree to StockX's terms of service. The individual is also provided a link to StockX's

[5] https://www.freep.com/story/money/business/2019/06/26/stockx-valuation-ceo-scott-cutler/1569408001/ (Last visited, August 2019) (Exhibit 3).

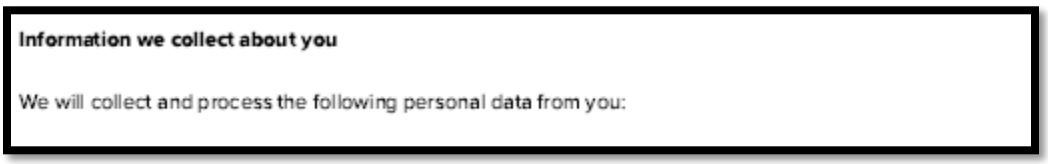
Privacy Policy. If the user chooses, he or she can open the Privacy Policy or Terms of Service by clicking on green hyperlinks, which launch separate windows displaying those forms, comprised of many pages of fine print.



20. Plaintiff, like all other members of the Class, created a user account on StockX's platform, and provided his first name, last name, username, email address, password, shoe size, and other information to StockX.

21. StockX's Privacy Policy is entitled "Your Privacy Rights." The current version of StockX's Privacy Policy as of the time of filing was last updated on October 9, 2018.

22. StockX fails to advise its users what information it does and will collect from them, even though it requires all prospective users to provide sensitive information at the very outset of their membership on the StockX platform. The first item listed in StockX's Privacy Policy purports to be information regarding "personal data" that StockX collects from its users; however, that section of the Privacy Policy is blank as shown in the below screen shot:


Information we collect about you

We will collect and process the following personal data from you:

As a result, even if the prospective user reviewed StockX's Privacy Policy, the user would not have been fully informed regarding StockX's actual privacy policy and practices with respect to the "personal data" collected by StockX when the user created an account.

23. Nevertheless, in its Privacy Policy, StockX assures its users that it protects their information on "secure servers" and claims that "[o]nce we have received your information, we will use strict procedures and security features to try to prevent unauthorised [sic] access."

III. StockX targets minors as part of its business model.

24. One of StockX's principal targeted demographics includes pre-teen and early-teen minors.

25. It is well-known that a large segment of StockX's user base is comprised of teenagers who have not yet reached the age of majority, and StockX has profited handsomely from their use of its services.[6]

26. The teenage demographic is a particularly active segment of StockX's user population — as teenagers are disproportionately likely to be among those highly passionate about amassing and collecting custom-made, ultrarare, vintage, and fashionable sneakers — and one of the main reasons for StockX's meteoric success.[7]

---

[6] https://www.businessinsider.com/teen-makes-money-selling-sneakers-stockx-2019-8 ("15-year-old Jake, whose last name has been omitted in order to protect his privacy, sells merchandise on the online sneaker resale marketplace StockX. Now a high school sophomore, he started reselling via Instagram when he was in eighth grade. Less than three years later, he says he's made over six figures.") (Last visited, August 2019) (Exhibit 4).

[7] https://finance.yahoo.com/news/american-teens-are-increasingly-becoming-sneakerheads-145501328.html ("American teenagers are embracing sneaker culture in significant numbers, according to Piper Jaffray's spring 2019 'Taking

27. On June 26, 2019, the Wall Street Journal published an article describing StockX as the "Latest $1 Billion Unicorn" and how StockX had "closed a round of venture funding that valued the startup at more than $1 billion" by "riding the sneaker-reselling craze **fueled by teens**."[8] And in an April 2019 article, Vox observed that "StockX has benefited from the rising popularity of acquiring tough-to-buy sneakers, especially among millennial men and **teenage boys."**[9]

28. According to a recent article in the New York Times, at the second annual "StockX Day" in April 2018, among the "rabid collectors" of StockX merchandise was "the 12-year-old son of a Venmo executive who had flown in for

---

Stock with Teens Survey.' Thirty-one percent of male teens and 22% of female teens consider themselves sneakerheads (sneaker enthusiasts or collectors). Teens surveyed own eight pairs of sneakers on average, and at least 30% buy a new pair every month.") (Last visited, August 2019) (Exhibit 5); https://www.nytimes.com/2018/01/04/insider/peak-sneaker-inside-sneaker-con.html ("[t]he heart and soul of the [Sneaker Con event sponsored by StockX] was the trading pit, an area in the back where a vibrant crowd of mostly teenage boys was talking and holding up sneakers, looking for buyers.") (Last visited, August 2019) (Exhibit 6); https://www.today.com/parents/sneakers-heart-sole-teen-boys-wbna36217370 ("What Imelda Marcos did with shoes, teenage boys do with sneakers.") (Last visited, August 2019) (Exhibit 7).

[8] https://www.wsj.com/articles/stockx-hub-for-sneakerheads-is-latest-1-billion-unicorn-11561571959 (Last visited, August 2019) (emphasis added) (Exhibit 8).

[9] https://www.vox.com/2019/4/19/18486120/stockx-billion-valuation-funding-dst-ggv-sneakerhead (Last visited, August 2019) (emphasis added) (Exhibit 9).

the event. To the crowd's delight, the 12-year-old scored an autographed LeBron James basketball jersey during a raffle."[10]

29. Indeed, Dan Gilbert, the billionaire founder of Quicken Loans, and co-founder of StockX, first began researching the business prospects of online sneaker culture and sales when he "noticed that his teenage son was flipping sneakers on eBay for profit."[11]

30. Gilbert personally acknowledged the importance of the teenage market to StockX's business strategy in an interview with Sole Collector back in February 2016, shortly after StockX was formed: "The amount of interest and activity among my boys and their friends about sneakers was just crazy," Gilbert said. "Then I start asking other people that have teenage boys, and it's almost 90-95 percent of the people that I asked said the same thing."[12]

[10] https://www.nytimes.com/2018/07/06/business/smallbusiness/stockx-sneakerheads-luxury-goods.html?smid=nytcore-ios-share&module=inline (Last visited, Aug. 6, 2019) (Exhibit 1).
[11] https://www.wsj.com/articles/this-website-is-the-stock-market-for-nikes-and-rolexes-1543251772 (Last visited, August 2019) (Exhibit 10).
[12] https://solecollector.com/news/2016/02/campless-stockx-dan-gilbert (Last visited, August 2019) (Exhibit 11).

31. StockX has become a "leading gauge of market value in the sneaker world" and now sponsors large trade shows to which teenage, and pre-teenage, kids flock.[13]

32. StockX specifically targets investors with "cultural cachet" among its young audience, including Eminem and the actor Mark Wahlberg.[14]

33. StockX also contains a link to its terms of service on the new user registration page. Buried in those terms of service, among many other fine-print details, is a forced-arbitration clause and class-waiver provision.

34. Based on their status as minors, Plaintiff and the Class are not bound by StockX's forced-arbitration and class-waiver provisions.

IV. Minors are a high-value target for cyber criminals and are particularly vulnerable to long-term identity theft and PII misuse.

35. According to numerous media reports and studies, stealing the identity of minors is especially attractive to cyber criminals for a host of reasons, including: (1) minors' credit reports are clean, which makes them particularly valuable; (2) minors do not check their credit reports or review monthly bills the way adults do; (3) thieves are more likely to have unfettered access to minors' identity and credit for

[13] https://www.freep.com/story/money/business/2018/07/09/detroit-stockx-sniffs-out-fake-sneakers/731070002/ ("Many in the crowd of buyers were teenage boys. Some looked no older than 12.") (Last visited, August 2019) (Exhibit 12).
[14] *Id.*

years or even decades; (4) it is often difficult or impossible to place a freeze on a minor's credit report—because they don't yet *have* credit; and (5) minors are less likely to receive notice, or to have an opportunity to take notice in the event that identity theft occurs or is ongoing, such as, e.g., if fraudulent accounts or charges occur under their names, if fake tax returns are filed in their names, if fraudulent health care is obtained under their identity, and if their information is fraudulently used in connection with employment.[15]

36. For these and other reasons, identity theft is a growing problem in the United States as it relates to our minor population. More than 1 million minors were victims of identity theft or fraud in 2017, totaling $2.6 billion in fraudulent activity.[16]

37. In fact, in 2017, among notified breach victims, 39% of minors became victims of actual fraud (as opposed to 19% of adults).[17]

38. According to a report on child identity theft published by Carnegie Mellon, a study based on identity protection scans of 40,000 U.S. children, the risk

[15] https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html (Last visited, August 2019) (Exhibit 13).
[16] https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html (Last visited, August 2019) (Exhibit 14). *See also* https://www.nbcnews.com/business/consumer/more-1-million-children-were-victims-id-theft-last-year-n885351 (Last visited, August 2019) (Exhibit 15).
[17] https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html (Last visited, August 2019) (Exhibit 15).

that someone was using their social security number was 51 times higher than the rate for adults in the same population, with the largest fraud being against a 16-year-old girl for $725,000.[18]

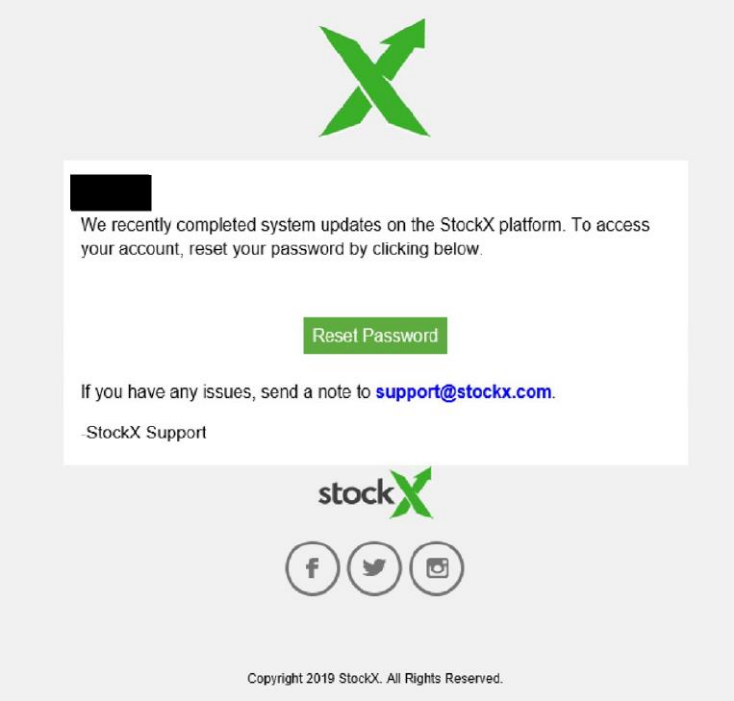
39. The Carnegie Mellon report continues: "[t]he potential impact [of identity theft] on the child's future is profound; it could destroy or damage a child's ability to win approval on student loans, acquire a mobile phone, obtain a job, or secure a place to live."[19]

40. Based on StockX's laser-focus on its young teenage demographic, StockX was well aware of the economic and reputational value of exploiting that market for its own monetary gain, and it should have been equally concerned with protecting the PII entrusted to it by that valuable and relatively defenseless group.

V. The data breach and StockX's attempted cover-up

41. On August 1, 2019, StockX sent its users, including Plaintiff and the Class, an email notification advising that StockX had "recently completed system updates on the StockX platform" and requiring them to reset their passwords.

[18] https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf, at PDF p. 4 (Last visited, August 2019) (Exhibit 16).
[19] https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf, at PDF p. 3 (Last visited, August 2019) (Exhibit 16).



42. This notification was based on a deception. In reality, StockX's password-reset notification was not a result of "system updates," as StockX falsely claimed; rather, StockX had experienced a data breach several months before the notification.

43. According to several news stories published on August 3, 2019—several days after StockX's fake "system updates" email—more than 6.8 million user accounts were stolen from StockX by a hacker in May 2019, who then listed the stolen data on the "dark web," an encrypted online area not indexed by conventional search engines that functions, in part, as a marketplace for thieves to buy and sell stolen PII.[20]

[20] *See* https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/ (Last accessed, August 2019) (Exhibit 17).

44. Information relating to this data breach was provided to TechCrunch, a media outlet emphasizing technology and cyber news, by an "unnamed data breached seller," who advised that the data was for sale on the dark web and provided TechCrunch with a sample of 1,000 records. Tech Crunch confirmed this information by contacting customers and providing them information from the stolen records that only the actual customers would know.[21]

45. Following publication of the news stories relating to the data breach, StockX sent a second email to its user base, acknowledging the data breach and admitting that the data breach was the real reason StockX had issued the previous password-reset email.

46. StockX further advised its users, including Plaintiff and the Class, that, according to then-known information, an unknown third-party had been able to gain access to certain customer data, including customer name, email address, shipping address, username, password, and purchase history.

47. On August 8, 2019, StockX sent another email to its users titled "Notice of Data Breach," stating that it was alerted to "suspicious activity potentially

[21] https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/ (Last visited, August 2019) (Exhibit 17).

involving customer data" on July 26, 2019—6 days before their false "system updates" email and 8 days before StockX apprised its users that it had been hacked.

48. The PII stolen from StockX constitutes "personal identifying information," which qualifies as "identity theft" when used to defraud or otherwise misrepresent with the intent of harming the owner of the information. Identity theft can occur by using (with the intent to defraud) information such as: name, birth date, address, telephone number, passwords, usernames, or other log-in information that can be used to access a person's electronic content, including content stored on a social networking site.[22]

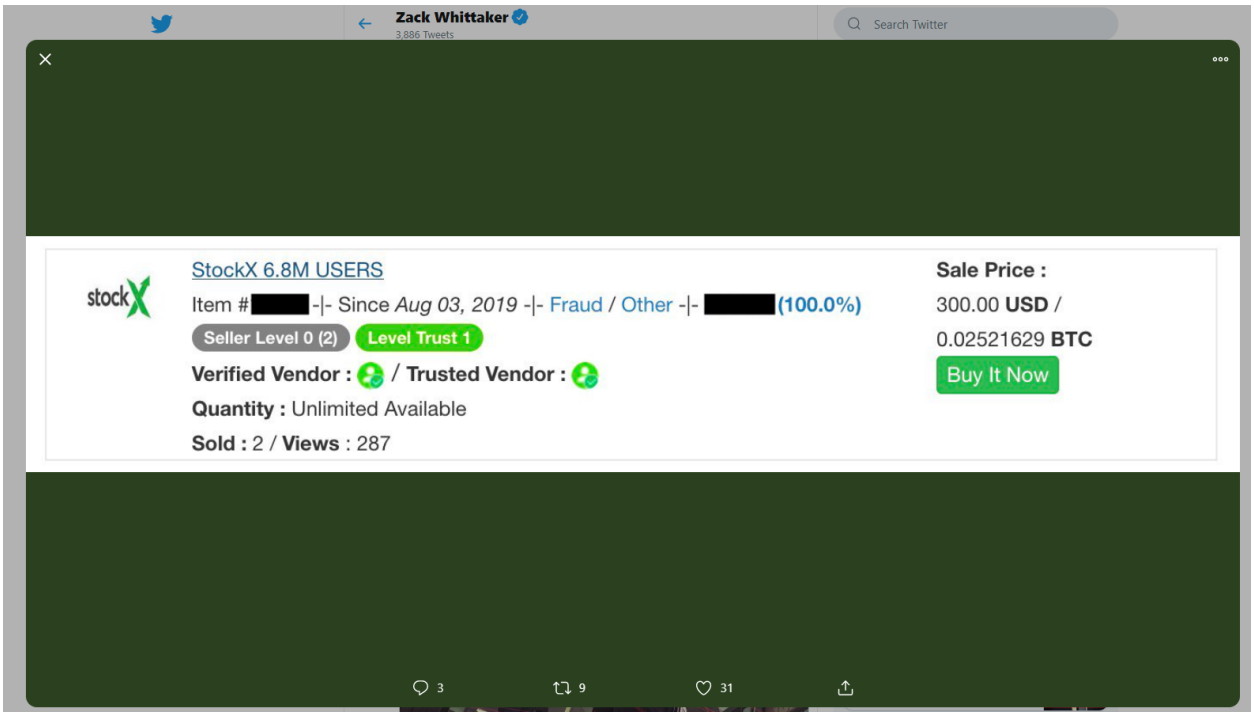
49. The information stolen from StockX included usernames and passwords—PII that is highly valued amongst cyber thieves and criminals on the Dark Web. For example, Apple ID usernames and passwords were sold on average for $15.39 each on the Dark Web, making them the most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for eBay ($12), Amazon (≤$10), and Walmart (≤$10) are not far behind.[23] In fact, there is a well-

[22] *See* K.S.A. 21-6107(2).

[23] https://fortune.com/2018/03/07/apple-id-dark-web-cost/ (Last visited, August 2019) (Exhibit 18). *See also* https://www.npr.org/2018/02/22/588069886/take-a-peek-inside-the-market-for-stolen-usernames-and-passwords (Last visited, August 2019) (Exhibit 19).

established market for stolen account credentials on the Dark Web, including StockX credentials.[24]

50. In early reports, prior to StockX notifying Plaintiff and the Class that their PII had been stolen, the StockX data had already been sold at least twice for $300 on the dark web.



51. Unsurprisingly, some users appear to have already been defrauded in the time between StockX's deceptive August 1 "system update" email and the August 3 email acknowledging that StockX had been hacked. One such user posted on Twitter

[24] https://krebsonsecurity.com/2017/12/the-market-for-stolen-account-credentials/ (Last visited, August 2019) (Exhibit 20); https://www.techradar.com/news/nearly-620-million-stolen-accounts-for-sale-on-dark-web (Last visited, August 2019) (Exhibit 21).

posted a screenshot of an allegedly fraudulent purchase for a Jordan 1 sneaker for more than $23,000 that occurred between the August 1 and August 3 emails from StockX.

52. On information and belief, it is not difficult to perceive one way in which criminals could leverage the stolen StockX data for a highly profitable enterprise. The criminals purchase the StockX data and thereby obtain Plaintiff's and the Class's stolen PII, including email address, usernames, passwords, shipping addresses, etc.; StockX sends its users a password-reset email based on its fake "system update" notice; the criminals trigger a password-reset through StockX's system and intercept the confirmation email by logging in to the user's email using the stolen StockX PII; and the criminal updates the StockX password and initiates fraudulent purchases redirecting either the funds, the merchandise, or both. This is but one example of many ways in which the stolen PII belonging to Plaintiff and the Class could be misused now and into the future.

53. The PII that Plaintiff and the Class entrusted to StockX has been stolen, sold, and purchased by criminals who will seek and have already sought to misuse it.

54. According to more recent reporting, bad actors "have already begun to decrypt the stolen passwords and it is expected for this information to be used in future attacks."[25]

55. The stolen information has also been added to the data breach monitoring website, "Have I Been Pwned,"[26] which added the StockX database to their website so users can check to see if their email was included in the breach. As shown in the below screenshot from "Have I Been Pwned," 6,840,399 accounts were stolen from StockX.

[25] https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/ (Last visited, August 2019) (Exhibit 22).
[26] https://haveibeenpwned.com/ (pronounced "poned") (Last visited, August 2019) (Front page of website attached as Exhibit 23, reference to StockX breach on PDF page 2).

56. A search of "Have I Been Pwned" confirms that Plaintiff's information was exposed as a result of the StockX data breach.[27]

57. Though originally being sold for $300, as referenced above, the username and password combinations are now being distributed on underground hacker forums for as little as $2.15, which virtually guarantees that it will be widely distributed. And for those cybercriminals who do not want to go through the trouble of decrypting the user accounts, they can purchase up to 367,000 decrypted accounts (of the more than 6.8 million stolen accounts) for $400.[28]

58. Now that the stolen data is available for a minimal sum, the credentials will be used in "credential stuffing" attacks, which involve thieves compiling and using usernames and passwords that were leaked from different data breaches to try and gain access to accounts at other sites.[29]

59. The founder of Rendition Infosec, a cybersecurity firm staffed by former NSA, DoD, and US Cyber Command Operators stated that StockX's misleading

[27] https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/ (Last visited, August 2019) (Exhibit 23).
[28] *Id.*
[29] https://www.wired.com/story/what-is-credential-stuffing/ (Last visited, August 2019) (Exhibit 24); https://www.bleepingcomputer.com/news/security/database-from-stockx-hack-sold-online-check-if-youre-included/ (Last visited, August 2019) (Exhibit 23).

conduct "robbed their users of the chance to evaluate their exposure" by not informing its users of the breach when it happened.[30]

60. Plaintiff's and the Class's PII was among the confidential information compromised in the StockX data breach, causing Plaintiff and the Class to suffer injury and damages, including but not limited to the improper disclosure of the PII, the loss of the value of the PII, ongoing disclosures and dissemination of the PII, the imminent threat of identity theft and other fraud against Plaintiff and the Class, the loss of Plaintiff's and the Class's privacy, and out-of-pocket expenses and time devoted to mitigating the effects of the data breach and ascertaining the extent of Plaintiff's and the Class's losses and exposure.

61. Plaintiff and the Class would never have provided their PII to StockX if it was known the security provided by StockX was not reasonable security or that StockX was not providing the security that StockX represented it would provide, as was revealed by the data breach described by media outlets following StockX's false "system updates" email.

[30] https://techcrunch.com/2019/08/03/stockx-hacked-millions-records/ (Last visited, August 2019) (Exhibit 17).

62. Plaintiff and the Class would further never have provided their PII to StockX if they had known that StockX would seek to deceive Plaintiff and the Class in the event that StockX was subject to a data breach.

63. Plaintiff and the Class would never have provided their PII to StockX if StockX had disclosed that it lacked adequate security measures and data security practices, as was revealed by the media reports.

64. Plaintiff and the Class have been damaged in that Plaintiff and the Class spent time and will spend additional time in the future speaking with representatives; researching and monitoring accounts; researching and monitoring credit history; responding to identity theft incidents; purchasing identity protection; and suffering annoyance, interference, and inconvenience, as a result of the data breach.

65. StockX's actions and failures to act when required have caused Plaintiff and the Class to suffer harm and face the significant and imminent risk of future harm, including:

- theft of their PII;
- costs associated with researching the scope and nature of the breach and of responding to the data breach and attendant risks and harm in light of StockX's misinformation campaign;

- costs associated with the detection and prevention of identity theft and unauthorized use of their PII;
- unauthorized access to and misuse of their online accounts;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the StockX data breach—including finding fraudulent charges and enrolling in and purchasing credit monitoring and identity theft protection services;
- the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals;
- damages to and diminution in value of their PII entrusted, directly or indirectly, to StockX with the mutual understanding that StockX would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; and
- continued risk of exposure to hackers and thieves of their PII, which remains in StockX possession and is subject to further breaches so long

as StockX fails to undertake appropriate and adequate measures to protect Plaintiff and the Class.

66. Consequently, Plaintiff and the Class are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the data breach and StockX's deceptive and unconscionable conduct.

CLASS ALLEGATIONS

67. Plaintiff brings this action on behalf of Plaintiff and those minors similarly situated both across the United States and within their State or Territory of residence.

68. Class certification is appropriate under Fed. R. Civ. P. 23(a) and (b)(1), (b)(2), and/or (b)(3).

69. **Nationwide Class:** All minor individuals in the United States whose PII was obtained or maintained by StockX and compromised as a result of the StockX data breach described herein.

70. **Numerosity (FRCP 23(a)(1)):** The class satisfies the numerosity requirement because it is composed of millions of persons, in numerous locations. The number of class members is so large that joinder of all its members is impracticable.

71. **Commonality and Predominance (FRCP 23(a)(2) and 23(b)(3)):** There are questions of law and fact common to the Class, and these questions predominate over questions affecting only individual Class members. Common legal and factual questions include, but are not limited to:

- whether the data breach constitutes a breach of the data-security commitments and obligations to protect and safeguard PII made to the Class by StockX in its privacy policy;
- whether StockX acted with intent or reckless indifference with respect to the Class and the safety, value, and security of the Class's PII when it falsely advised the Class that a password reset was required because of a "system update," not a data breach, which StockX knew to be the case at the time of its statements;
- whether StockX was negligent in its representations to the Class concerning its security protocols;
- whether StockX's conduct and practices described herein amount to acts of intrusion upon seclusion under the laws of the "Intrusion Upon Seclusion States" defined below;
- whether StockX was negligent in making misrepresentations to the Class when it falsely advised the Class that a password reset was

required because of a "system update," not a data breach, which StockX knew to be the case at the time of its statements;

- whether StockX was negligent in establishing, implementing, and following security protocols;
- whether StockX failed to abide by all applicable legal requirements (including relevant state law requirements) and industry standards concerning the privacy and confidentiality of the Class members' PII;
- whether the Class members' PII was compromised and exposed as a result of the data breach and the extent of that compromise and exposure;
- whether the Class members are entitled to compensatory damages; and
- whether the Class members are entitled to punitive damages.

72. **Typicality (FRCP 23(a)(3):** Plaintiff's claims are typical of the claims of the members of the Class because Plaintiff's claims, and the claims of all Class members, arise out of the same conduct, policies, and practices of StockX, as alleged herein, and all members of the Class are similarly affected by StockX's wrongful conduct and the data breach described herein.

73. **Adequacy of Representation (FRCP 23(a)(4)):** Plaintiff will fairly and adequately represent the Class and have retained counsel competent in the

prosecution of class action litigation; data breach litigation; data privacy and cybersecurity law; and technical I.T. concepts, practices, and theory. Plaintiff has no interests antagonistic to those of other members of the Class. Plaintiff is committed to the vigorous prosecution of this action and anticipates no difficulty in the management of this litigation as a class action.

74. Class action status in this action is warranted under Rule 23(b)(1)(A) because prosecution of separate actions by the members of the Class would create a risk of establishing incompatible standards of conduct for Defendants. Class action status is also warranted under Rule 23(b)(1)(B) because prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

75. In the alternative, certification under Rule 23(b)(2) is warranted because Defendants acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive, declaratory, or other appropriate equitable relief with respect to the Class as a whole.

76. In the alternative, certification under Rule 23(b)(3) is appropriate because questions of law or fact common to members of the Class predominate over

any questions affecting only individual members, and class action treatment is superior to the other available methods for the fair and efficient adjudication of this controversy.

CAUSES OF ACTION AND CLAIMS FOR RELIEF

COUNT I — Negligence
(On behalf of Plaintiff and the Class)

77. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

78. StockX owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing their PII that StockX collected.

79. StockX owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII that StockX collected.

80. StockX owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the Class of a data breach as soon as possible after it is discovered.

81. StockX owed a duty of care to Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

82. StockX solicited, gathered, and stored the PII provided by Plaintiff and the Class.

83. StockX knew or should have known it inadequately safeguarded this information.

84. StockX knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiff and the Class, and StockX was therefore charged with a duty to adequately protect this critically sensitive information.

85. StockX had a special relationship with Plaintiff and the Class. Plaintiff's and the Class's willingness to entrust StockX with their PII was predicated on the understanding that StockX would take adequate security precautions. Moreover, only StockX had the ability to protect its systems and the PII it stored on them from attack.

86. StockX's own conduct also created a foreseeable risk of harm to Plaintiff and the Class and their financial information. StockX's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

87. StockX breached its duties to Plaintiff and the Class by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the financial information of Plaintiff and the Class.

88. StockX breached its duties to Plaintiff and the Class by creating a foreseeable risk of harm through the misconduct previously described.

89. StockX breached the duties it owed to Plaintiff and the Class by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.

90. StockX breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose that Plaintiff's and the Class members' PII had been improperly acquired or accessed.

91. The law further imposes an affirmative duty on StockX to timely disclose the unauthorized access and theft of the financial information to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their financial information.

92. StockX breached its duty to notify Plaintiff and the Class by failing to provide Plaintiff and the Class information regarding the breach until August 3, 2019. To date, StockX has not provided sufficient information to Plaintiff and the Class

regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

93. As a direct and proximate result of StockX's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – Negligent Misrepresentation
(On behalf of Plaintiff and the Class)

94. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

95. Through its Privacy Policy and other actions and representations, StockX held itself out to Plaintiff and the Class as possessing and maintaining adequate data security measures and systems that were sufficient to protect the PII belonging to Plaintiff and the Class.

96. StockX knew or should have known that it was not in compliance with the representations made in its Privacy Policy.

97. StockX knowingly and deliberately failed to disclose material weaknesses in its data security systems and procedures that good faith and common decency required it to disclose to Plaintiff and the Class.

98. Neither Plaintiff nor the Class could have known or discovered the material weaknesses in StockX's data security practices.

99. A reasonable business would have disclosed information concerning material weaknesses in its data security measures and systems to Plaintiff and the Class.

100. StockX also failed to exercise reasonable care when it falsely conveyed information to Plaintiff and the Class on August 1, 2019, relating to the underlying need for Plaintiff and the Class to reset their passwords, which misrepresentation failed to sufficiently convey the facts underlying the actual need for a password reset; failed to instill the urgency of the need to reset their passwords immediately; provided the thieves of the stolen information with additional time and cover to further purloin and re-sell the stolen PII belonging to Plaintiff and the Class; provided the thieves and the purchasers of the stolen information with an opportunity to directly defraud Plaintiff and the Class; and failed to adequately apprise Plaintiff and the Class of the fact that their PII was compromised and in imminent jeopardy of falling further into the hands of cyber criminals.

101. StockX also failed to exercise reasonable care when it failed to timely communicate information concerning the data breach that it knew, or should have known, compromised PII of Plaintiff and the Class.

102. Plaintiff and the Class relied on Capital One's representations, or lack thereof, when they provided their PII to StockX.

103. As a direct and proximate result of StockX's negligent misrepresentations by omission, Plaintiff and the Class have suffered injury, have been damaged as described herein, and are entitled to damages in an amount to be proven at trial.

COUNT III – Fraud and fraud through silence
(On behalf of Plaintiff and the Class)

104. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

105. StockX knew that data belonging to Plaintiff and the Class had been stolen prior to its false "system update" email on August 1, 2019. This knowledge was of material importance relating to the safety, value, and security of the PII belonging to Plaintiff and the Class.

106. Plaintiff and the Class did not know about the theft of their PII from StockX, nor could they have discovered such information by exercise of reasonable diligence.

107. StockX was under an obligation to forthrightly and promptly communicate the pertinent facts relating to the data breach to Plaintiff and the Class to permit them to undertake appropriate protective measures to mitigate the harm caused by StockX's failure to adequately protect the data and to reasonably safeguard their identities, livelihood, and safety.

108. Despite its knowledge of the data breach and the imminent danger the PII theft posed, StockX failed to timely and forthrightly advise Plaintiff and the Class of the breach; instead, StockX falsely advised Plaintiff and the Class that a password reset was necessary because of "system upgrades."

109. In conjunction, and simultaneous with its misrepresentations relating to the need for Plaintiff and the Class to reset their passwords, StockX intentionally failed to communicate to Plaintiff and the class material facts relating to the data breach, the theft of their PII, the urgency with which Plaintiff and the Class needed to update their passwords, the concurrent and urgent need for Plaintiff and the Class to protect and safeguard their data, and other measures needed in light of the data breach.

110. Plaintiff and the Class justifiably relied on StockX's misrepresentations and StockX's intentional withholding of material facts, suffered injuries as a result, and were damaged as discussed herein and as will be proven at trial.

111. As a direct result of StockX's fraud and fraud by silence, Plaintiff and the Class have suffered injury, have been damaged as described herein, and are entitled to damages in an amount to be proven at trial.

COUNT IV – Negligence Per Se – FTC Act
(On behalf of Plaintiff and the Class)

112. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

113. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as StockX of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Equifax's duty.

114. StockX violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII; by failing to comply with applicable industry standards; by falsely representing to its users and the public the nature and scope of the data breach and the need for password resets; and by unduly delaying reasonable notice of the actual breach. StockX's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a data breach, and the foreseeable consequences of misleading its users and the public.

115. StockX's violation of Section 5 of the FTC Act constitutes negligence per se.

116. Plaintiff and the Class are within the category of persons the FTC Act was intended to protect.

117. The harm that occurred as a result of the data breach described herein and in the various media reports detailing StockX's deception relating to the data breach is the type of harm the FTC Act was intended to guard against.

118. As a direct and proximate result of StockX's negligence per se, Plaintiff and the Class have suffered injury, have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in StockX's possession, and are entitled to damages in an amount to be proven at trial.

COUNT V – Unjust Enrichment
(On behalf of Plaintiff and the Class)

119. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

120. Plaintiff and the Class have an interest, both equitable and legal, in their PII that was collected and maintained by StockX. This PII was conferred on StockX directly by Plaintiff and the Class themselves.

121. StockX was benefitted by the conferral upon it of the PII pertaining to Plaintiff and the Class and by its ability to retain and use that information. StockX understood that it was in fact so benefitted.

122. StockX also understood and appreciated that the PII pertaining to Plaintiff and the Class was private and confidential and its value depended upon StockX maintaining the privacy and confidentiality of that PII.

123. But for StockX's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and the Class would not have transferred PII to StockX or entrusted their PII to StockX, and StockX would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers and users of its platform, gaining the reputational advantages conferred upon it by Plaintiff and the Class, collecting excessive sales commissions as described herein, raising investment capital as described herein, and realizing excessive profits.

124. As a result of StockX's wrongful conduct as alleged in this Complaint (including, among other things, its deception of Plaintiff, the Class, its users in general, and the public relating to the nature and scope of the data breach; its utter failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to Plaintiff and the Class without having adequate data security measures; and its other conduct facilitating the theft of that PII) StockX has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

125. StockX's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

126. Under the common law doctrine of unjust enrichment, it is inequitable for StockX to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. StockX's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

127. The benefit conferred upon, received, and enjoyed by StockX was not conferred officiously or gratuitously, and it would be inequitable and unjust for StockX to retain the benefit.

128. StockX is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on StockX as a result of its wrongful conduct, including specifically the value to StockX of the PII that was stolen in the StockX data breach and the profits StockX is receiving from the use and sale of that information.

COUNT VI – Violation of State Data Breach Statutes
(On behalf of Plaintiff and all members of the Class residing in states with applicable data breach statutes)

129. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

130. StockX is in possession of PII belonging to Plaintiff and the Class and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

131. StockX failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by the laws of the State of Kansas, Michigan, and all other applicable State laws.

132. StockX further failed to provide reasonable and timely notice of the data breach to Plaintiff and the Class as required by the various state data breach notification statutes, including, without limitation, K.S.A. 50-7a01, *et seq*.

133. As a result of StockX's failure to reasonably safeguard the PII belonging to Plaintiff and the Class, and StockX's failure to provide reasonable and timely notice of the data breach to Plaintiff and the Class, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in StockX's possession, and are entitled to damages in an amount to be proven at trial.

COUNT VII – Intrusion Upon Seclusion
(On behalf of Plaintiff and all members of the Class who reside in Intrusion Upon Seclusion States)

134. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

135. Plaintiff brings this claim on behalf of persons who reside in the following states: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia (the "Intrusion Upon Seclusion States").

136. Plaintiff had a reasonable expectation of privacy in the PII Defendant mishandled.

137. By failing to keep Plaintiff's Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant invaded Plaintiff's privacy by:

- Intruding into Plaintiff's private affairs in a manner that would be highly offensive to a reasonable person; and

- Publicizing private facts about the Plaintiffs, which is highly offensive to a reasonable person.

138. StockX knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider StockX's actions highly offensive.

139. StockX invaded Plaintiff's right to privacy and intruded into Plaintiff's private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

140. As a proximate result of such misuse and disclosures, Plaintiff's reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. StockX's conduct amounted to a serious invasion of Plaintiff's protected privacy interests.

141. In failing to protect Plaintiff's Private Information, and in misusing and/or disclosing their Private Information, StockX has acted with malice and oppression and in conscious disregard of Plaintiff's and the Class Members' rights to have such information kept confidential and private. The Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of Plaintiff and the Class.

COUNT VIII – Declaratory Judgment
(On behalf of Plaintiff and the Class)

142. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

143. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

144. An actual controversy has arisen in the wake of the StockX data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether StockX is currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their PII. Plaintiff allege that StockX's data security measures remain inadequate.

145. Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

146. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that StockX continues to owe a legal duty to secure

consumers' PII and to timely notify consumers of any data breach and that StockX is required to establish and implement data security measures that are adequate to secure consumers' PII.

147. The Court also should issue corresponding prospective injunctive relief requiring StockX to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

148. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury, and Plaintiffs and the Class lack an adequate legal remedy. The threat of another StockX data breach is real, immediate, and substantial. If another breach at StockX occurs, Plaintiff will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

149. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to StockX if an injunction is issued. Among other things, if another massive data breach occurs at StockX, Plaintiff will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to StockX of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and StockX has a pre-existing legal obligation to employ such measures.

150. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at StockX, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of members of the Class, as applicable, respectfully requests that the Court enter judgment in their favor and against StockX, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

2. That Plaintiff be granted the declaratory relief sought herein;

3. That the Court grant permanent injunctive relief to prohibit StockX from continuing to engage in the unlawful acts, omissions, and practices described herein;

4. That the Court award Plaintiff and Class and Class members compensatory, consequential, and general damages in an amount to be determined at trial;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

7. That the Court award pre- and post-judgment interest at the maximum legal rate; and

8. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution.

9. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demand a jury trial on all claims so triable.

Dated: August 19, 2019

Respectfully submitted,

*/s/ E. Powell Miller*_____

E. Powell Miller (P39487)
Sharon S. Almonrode (P33938)
William Kalas (P82113)
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Suite 300
Rochester, Michigan 48307
Telephone: (248) 841-2200
Fax: (248) 652-2852
epm@millerlawpc.com
ssa@millerlawpc.com
wk@millerlawpc.com

FOULSTON SIEFKIN LLP
Scott C. Nehrbass
Daniel J. Buller
32 Corporate Woods, Suite 600
9225 Indian Creek Parkway
Overland Park, KS 66210-2000
Tel: (913) 253-2144
Fax:(866) 347-1472
snehrbass@foulston.com
dbuller@foulston.com

FOULSTON SIEFKIN LLP
Boyd A. Byers
1551 N. Waterfront Parkway, Suite 100
Wichita, Kansas 67206-4466
Tel: (316) 291-9796
Fax: (866) 559-6541
bbyers@foulston.com

ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS